UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/662,072	09/14/2000	John Border	10792-1148	1446

30671 7590 07/16/2012

DITTHAVONG MORI & STEINER, P.C.
918 Prince Street
Alexandria, VA 22314

EXAMINER	
EL CHANTI, HUSSEIN A	
ART UNIT	**PAPER NUMBER**
3663	

NOTIFICATION DATE	DELIVERY MODE
07/16/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket@dcpatent.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JOHN BORDER and MATTHEW BUTEHORN

Appeal 2010-003698
Application 09/662,072
Technology Center 2400

Before ALLEN R. MACDONALD, KRISTEN L. DROESCH, and LARRY J. HUME, *Administrative Patent Judges*.

HUME, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE [1]

Introduction

This is a decision on appeal under 35 U.S.C. § 134(a) of the rejection of claims 3, 5-9, 11-29, 32, 34-38, and 40-59. We have jurisdiction under 35 U.S.C. § 6(b).

Exemplary Claim

Exemplary independent claim 32 under appeal reads as follows (***emphasis*** added to contested limitation):

> 32. A method for providing data communication with a plurality of network entities, comprising:
>
> facilitating communication with the network entities by performing at least one performance enhancing function;
>
> communicating with the network entities via a first type of connection and a second type of connection;
>
> establishing multiple connections of the first type associated with different applications;
>
> intercepting and altering a data flow within one of the connections to add to or delete from the data flow to reduce startup latency;
>
> spoofing only connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired; and
>
> ***selectively multiplexing the spoofed connections onto a single connection of the second type***.

[1] Throughout this Decision, we refer to the Final Office Action (FOA) mailed Jul. 29, 2008; the Appeal Brief (App. Br.) filed Feb. 2, 2009; and the Examiner's Answer (Ans.) mailed June 9, 2009.

Prior Art

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Yates	US 6,167,438	Dec. 26, 2000 (filed May 22, 1997)

Rejection on Appeal

The Examiner rejected claims 3, 5-9, 11-29, 32, 34-38, and 40-59 under 35 U.S.C § 102(e) as being anticipated by Yates (FOA 2; Ans. 3).

Appellant's Contention

In the Appeal Brief, Appellants contend that the Examiner erred in rejecting claim 32 as follows:

> Independent claim 32 recites, inter alia, "selectively multiplexing the spoofed connections onto a single connection of the second type." These features are not disclosed in *Yates et al.*
>
> The Examiner, in the Final Office Action, contends that such features are taught in *Yates et al.* at col. 9, line 54-col. 10, line 15. This portion of *Yates et al.* provides as follows:
>
> > To overcome this hurdle, in the preferred embodiment, intermediate routers 14 have some awareness of the TCP protocol. TCP aware routers 14 are able to detect TCP connection requests to all HTTP servers (i.e., a {SYN} packet directed to the HTTP port), and have the ability to act as a proxy for, or "spoof" the home server 20.
> >
> > This functionality is implemented by the snooper 28. In particular, snoopers 28 located in routers 14 on the path to a home server 20 inspect packets that fly-by, identify such packets, and intercept any {SYN}

> packets directed to HTTP home servers 20. As {SYN} packets do not contain any information identifying which document the client 12 intends to request, the snooper 28 acts as a proxy for, or "spoofs" the home server 20, by establishing a connection between the client 12 and the local transport layer in the cache server 16, and noting the initial sequence numbers used by both the client 12 and the local transport layer.
>
> After the connection is established the snooper 28 inspects all packets that fly-by, and waits for the corresponding {GET} request. Once the {GET} request arrives the snooper 28 queries the local filter 26 and the resource manager 24 to determine if the requested document is cached. If the document is cached the snooper 28 forwards the HTTP {GET} message to the local resource manager 24, waits for the resource manager 24 to service the request, and then terminates the connection.
>
> Otherwise, the requested document is not cached (i.e., the filter 26 or resource manager 24 missed). Several different approaches may be taken to servicing the document request at this point.

As is clear from this passage of *Yates et al.*, and the remainder of the reference, there is no multiplexing operation, particularly in the manner claimed, disclosed. While the cited passage indicates that multiple TCP/IP connections may be established with home server 20, neither the home server nor any other element within Yates et al., multiplexes these connections.

At page 8 of the Final Office Action, the Examiner equates the plurality of TCP connection requests received by the router in Yates et al. to the claimed connections of the "first type" and equates the connection between the client and the local transport layer established by the home server as the claimed "second type" of connection. Respectfully, this rationale is flawed.

> Appellants do not gainsay that TCP connections in *Yates et al.* may be interpreted as a "first type" of connection. However, in accordance with the language of claims 3 and 32, there must be "a multiplexing element configured to selectively multiplex the spoofed connections onto a single connection of the second type" and "selectively multiplexing the spoofed connections onto a single connection of the second type," respectively. The snooper 28 of *Yates et al.* provides no multiplexing function. Rather, the snoopers 28 are located in the routers 14 on the path to the home server 20 and the snoopers inspect packets that fly-by, identify those packets and intercept certain packets, viz., those packets that do not identify a document the client intends to request. The snooper acts as a proxy for the home server by establishing a connection between the client and the local transport layer in a cache server 16. It is only after this connection is established that the snooper inspects all packets that fly-by, waiting for a corresponding request to retrieve a document. However, this "spoofed" connection between the client and the local transport layer in the cache server is not "multiplexed" and clearly is not "multiplexed . . . onto a single connection of the second type."

App. Br. 5-7 (emphasis omitted).

Issue on Appeal

Did the Examiner err in rejecting claims 3, 5-9, 11-29, 32, 34-38, and 40-59 as being anticipated because Yates does not disclose the argued limitation?

ANALYSIS

We agree with Appellants' above-cited contentions.

CONCLUSIONS

(1) Appellants have established that the Examiner erred with respect to the rejection of claims 3, 5-9, 11-29, 32, 34-38, and 40-59 under 35 U.S.C. § 102(e).

(2) On this record, claims 3, 5-9, 11-29, 32, 34-38, and 40-59 have not been shown to be anticipated.

DECISION

The Examiner's rejection of claims 3, 5-9, 11-29, 32, 34-38, and 40-59 is reversed.

REVERSED

tj